Leakthemall

Leakthemall Ransomware

(шифровальщик-вымогатель) (первоисточник)

[Translation into English]

Этот крипто-вымогатель шифрует данные пользователей с помощью инструмента шифрования **Lockdown**, а затем требует связаться с вымогателями, что заплатить за ключ дешифрования и вернуть файлы.
Оригинальное название: в записке не указано. На файле написано: win.exe. Для Windows x64. Написан на языке Go. Разработчик (пользователь ПК): Amir.

Обнаружения:

DrWeb -> Trojan.Encoder.32463
BitDefender -> Trojan.GenericKD.43776492
ESET-NOD32 -> Win64/Filecoder.CE
Kaspersky -> Trojan-Ransom.Win32.Crypren.ahfl
Malwarebytes -> Ransom.FileCryptor
Symantec -> Downloader
TrendMicro -> Ransom_Crypen.R002C0DI520

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

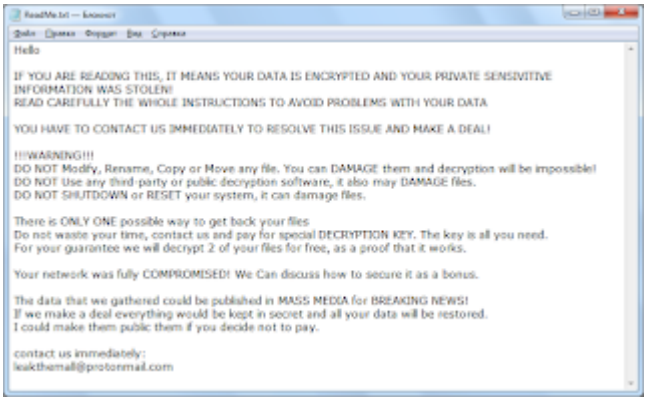
© Генеалогия: неизвестный код > LeakTheMall

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.crypt** **Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на начало сентября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **ReadMe.txt**



Содержание записки о выкупе:

Hello
IF YOU ARE READING THIS, IT MEANS YOUR DATA IS ENCRYPTED AND YOUR PRIVATE SENSIVITIVE INFORMATION WAS STOLEN!
READ CAREFULLY THE WHOLE INSTRUCTIONS TO AVOID PROBLEMS WITH YOUR DATA
YOU HAVE TO CONTACT US IMMEDIATELY TO RESOLVE THIS ISSUE AND MAKE A DEAL!
!!!WARNING!!!
DO NOT Modify, Rename, Copy or Move any file. You can DAMAGE them and decryption will be impossible!
DO NOT Use any third-party or public decryption software, it also may DAMAGE files.
DO NOT SHUTDOWN or RESET your system, it can damage files.
There is ONLY ONE possible way to get back your files
Do not waste your time, contact us and pay for special DECRYPTION KEY. The key is all you need.
For your guarantee we will decrypt 2 of your files for free, as a proof that it works.
Your network was fully COMPROMISED! We Can discuss how to secure it as a bonus.
The data that we gathered could be published in MASS MEDIA for BREAKING NEWS!
If we make a deal everything would be kept in secret and all your data will be restored.
I could make them public them if you decide not to pay.
contact us immediately:
leakthemall@protonmail.com

Перевод записки на русский язык:

Привет

ЕСЛИ ВЫ ЧИТАЕТЕ ЭТО, ЗНАЧИТ ВАШИ ДАННЫЕ ЗАШИФРОВАНЫ И ВАША ЧАСТНАЯ ИНФОРМАЦИЯ УКРАДЕНА!

ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ВСЕ ИНСТРУКЦИИ, ЧТОБЫ ИЗБЕЖАТЬ ПРОБЛЕМ С ВАШИМИ ДАННЫМИ

ВЫ ДОЛЖНЫ СВЯЗАТЬСЯ С НАМИ НЕМЕДЛЕННО, ЧТОБЫ РАЗРЕШИТЬ ЭТОТ ВОПРОС И ЗАКЛЮЧИТЬ СДЕЛКУ!

!!!ПРЕДУПРЕЖДЕНИЕ!!!

ЗАПРЕЩАЕТСЯ изменять, переименовывать, копировать и перемещать какие-либо файлы. Вы можете их ПОВРЕДИТЬ и расшифровка будет невозможна!

НЕ ИСПОЛЬЗУЙТЕ сторонние или общедоступные программы для дешифрования, они также могут ПОВРЕДИТЬ файлы.

НЕ ВЫКЛЮЧАЙТЕ и НЕ ПЕРЕЗАГРУЖАЙТЕ систему, это может повредить файлы.

Есть ТОЛЬКО ОДИН способ вернуть свои файлы

Не теряйте время, свяжитесь с нами и оплатите специальный КЛЮЧ ДЕШИФРОВАНИЯ. Ключ - это все, что вам нужно.

Для вашей гарантии мы бесплатно расшифруем 2 ваших файла как доказательство того, что это работает.

Ваша сеть полностью СКОМПРОМИТИРОВАНА! Мы можем обсудить, как обезопасить её, как бонус.

Собранные нами данные могут быть опубликованы в СМИ для ГЛАВНЫХ НОВОСТЕЙ!

Если мы заключим сделку, все будет в секрете и все ваши данные будут восстановлены.

Я могу обнародовать их, если вы не заплатите.

срочно напишите нам:

leakthemall@protonmail.com

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

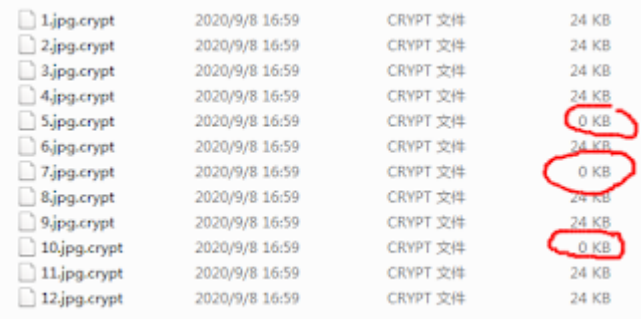
Нужно всегда использовать Актуальную антивирусную защиту!!!

Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

Список файловых расширений, подвергающихся шифрованию:

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Согласно сообщению исследователя вредоносных программ **xiaopao**, вместо шифрования файлы повреждаются и получают размер 0 Kb.



Файлы, связанные с этим Ransomware:
ReadMe.txt - название файла с требованием выкупа
win.exe - название вредоносного файла
Использует **Lockdown** и **MemGuard**

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:

Email: leakthemall@protonmail.com
BTC: -
Github-URL: hxxxs://github.com/raz-varren/lockdown
Github-URL: hxxxs://github.com/awnumar/memguard
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
🔻 **Triage analysis >>**
Ⓗ **Hybrid analysis >>**
Σ VirusTotal analysis >>
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
⩓ MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

??? Обновление от 19 сентября 2020:

Расширение: **.montana**

Email: montanarecover@aol.com, montanarecover@cock.li

Записка: !HELP!.txt

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Read to links:
Tweet on Twitter + Tweet + myTweet
ID Ransomware (ID as Leakthemall)
Write-up, Topic of Support
*

Thanks:
M. Shahpasandi, Michael Gillespie
Andrew Ivanov (author)
xiaopao
to the victims who sent the samples
